પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક
Question Sub-question No.

Q. 0 1 Answer Any Seven.

Q-1 Define Plaintext and cipher text.

Ans-1 Plain text - Plain text means an unencrypted message or information information pending input into crypto graphic algorithm.

Cipher text - It is an algorithm method that replaces the Plaintext into decrypted message.

Q-3 List out the types of Crypt analysis attack ?

Ans-3. Types of Cryptanalysis attack :-

(i) Known-Plaintext Analysis (KPA)
(ii) Chosen-Plaintext Analysis (CPA)
(iii) Ciphertext-only Analysis (COA)
(iv) Man-In-The-Middle attack (MITM)
(v) Adaptive chosen-Plaintext Analysis (ACPA).

Question / Sub-question No.

[ ] + [ ] + [ ] + [ ] = [ ]

Q. 0 4 List out any four goal of OS Hardening?

Ans-4 Goal of OS Hardening-

- Encrypting the HDD or SSD that stores and hosts your OS
- Removing unnecessary drivers
- Enabling and configuring secure boot
- Limiting and authenticating system access permissions.

Q-5 Define transposition technique

Ans-5 In transposition technique, we do not simply replace one alphabet with another, we do rearrangment & perform some permutation over the plaintext alphabets is known as transposition technique.

Q-8 List out OS security assesment tool.

Ans-8 Nessus (windows, Linux)

Saint (Linux, open source).

પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક
Question Sub-question No.

Q. 6 Define transposition technique.

Ans 6 (i) $[(a \bmod n) + (b \bmod n)] \bmod n = (a+b) \bmod n$

(ii) $[(a \bmod n) - (b \bmod n)] \bmod n = (a-b) \bmod n$

(iii) $[(a \bmod n) * (b \bmod n)] \bmod n = (a \times b) \bmod n$.

Q-9 What is Block size of plain text and numbers of rounds in DES algorithm?

Ans-9 The block size of Plain text is 64 bit and number of rounds in DES algorithm. is 16 round

---

પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક Question Sub-question No.	[ ] + [ ] + [ ] + [ ] = [ ]

Q.02

Q-A Describe Data Integrity:-

Ans-A
- As with confidentiality, integrity can apply to a stream of message, a single message or selected fields within a message.
- Assures that message are received as sent with no duplication, insertion, modification, recording or replays.
- The destructor of data is also covered under this service.
- Data Integrity refers to reliability and trustworthiness of data throughout its lifecycle.

Q-B Explain Confidentiality and access control?

Ans-B Confidentiality-

- Confidentiality is a Protection of transmitted data from Passive attacks.
- with respect to the content of data transmission several level of Protection can be identified.
- The other aspect of confidentiality is the Protection of traffic flow from the analysis.

પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક
Question
Sub-question No.

☐ + ☐ + ☐ + ☐ = ☐

Q.___

- It requires that an attacker not be able to observe the source and destination and characteristics of communication.

* Access Control:-

- Access control is the ability to limit & control the access to host system and application via communication link to achieve this, each entity trying to gain access must be identified or authenticated.

- Through authentication and authorization access control Policies make sure users are who they say they are and that they have appropriate access to company data.

- Access control can be applied to limit Physical access to campuses, building, rooms, and data centres.

Q-C Explain Active Security attacks:-

Ans-c By using Active attack modification and creation of the false message is Possible.

- An unauthorized user is able to read as well as modify the message.

Q.___ (i) Masquerade :-

- In masquerade attack, attacker enters to the Network and send a message to receiver with identification of the Authorized Sender.

- So when message is received by reciever, the reciever thinks that its from a correct Source

(ii) Release of message Content :-

- In this attack, the attacker capture the original message from sender, and able to modify some portion of the message or create a new message and send the updated message to reciever.

(iii) Replay :-

- In this attack, the attacker capture the message which is transmitted from sender, and later on resend the message to the receiver.

(iv) Denial of Services

- This attack, may have a specific target, Attacker send, all the message to particular destination.

Explain Passive Security attack:-

Passive attack:-

- In Passive attack an unauthorized Party can achieve the data by constantly monitoring the transmitted message

- The goal is getting the transmitted message

- In Passive attack, the 3rd Party can only read the message, not able to modify the message.

* Types of Passive attack

(i) Release of of message content:-

- In this attack, an attacker can simply read the message from sender to receiver.

(ii) Traffic analysis -

- An opponent can able to observe the Pattern of ~~mes~~ message. the attacker could determine the ~~message~~ location. and identification of Sender ~~and~~ receiver

પ્રશ્ન / પેટાપ્રશ્ન ક્રમાંક
Question Sub-question No.

[ ] + [ ] + [ ] + [ ] = [ ]

Q. 0 3

Q-A Explain rail fence technique

Ans-A Rail Fence is an example of transposition technique.

- In Rail Fence write down the plain text message as a sequence of diagonals.

- Then, read the plain text.

Ex:- Plain text :- Hello world

```
H   l   o   o   l
  e   l   w   r   d
```

- After we arrange the plaintext in diagonal form it would look like this

- Now we have to read it by row and write in sequence

- So we have, Hlool elwrd as our ciphertext

- The elements are just rearranged not replaced.

- The rail fence technique works by writing your message on alternate lines across the page, and then reading off each line.

પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક Question Sub-question No.

Q-B Explain Diffie-Hellman key exchange algorithm?

Ans-B A user A and user B wants to share a secret key. but in secure communication every piece of information that they exchange is observed by another user C.

- Firstly A and B have to agree on a large Prime number p and q, non-zero value g.

- Then for A pick a secret integer (a). that keeps secret at same time B also selects a secret integer (b) that also secret

- A user computes this, $VA = g^a \bmod P$

- B user computes this, $VB = g^b \bmod P$

- Then they exchange the computed values user A sends (VA) to user B and user B sends value (VB) to user A.

- Finally, user A & user B again uses their secret integer to compute.

Q.

→ User A computes as :-

$$V_A' = V_B^a \bmod P$$
$$= (g^b \bmod P)^a \bmod P$$
$$= (g^b)^a \bmod P$$
$$= g^{ba} \bmod P$$
$$= g^{ab} \bmod P$$
$$= (g^a \bmod P)^b \bmod P$$
$$= V_A^b \bmod P$$

Q-C Explain columnar transposition technique with Example.

Ans-C The columnar transposition cipher is a form of transposition cipher. Just like rail fence cipher. columnar involves writing the plaintext out in rows, and then reading the ciphertext off in columns one by one

- The columnar transposition rearranges the plaintext letters, based on a matrix filled with letters in order determined by the secret keyword

Q.

- For Example

 - Let's encryp. a message "A midsummer Night's Dream", we will use the secret key as mentioned above. The number sequence derived from this keyword is 6723154, so matrix created for encryption will have seven columns.

6	7	2	3	1	5	4
A	M	I	D	S	U	M
M	E	R	N	I	G	H
T	S	D	R	E	A	M.

Cipher text is:- SIE IRD DNR MHM UGA AMT MES

Q-4 Explain Play fair Cipher technique with example?

Ans-4. The Playfair algorithm is based on 5X5 matrix of letters constructed using a keyword

- The matrix is Generated by falling the letters of keywords left to right & top to bottom.

Q.

- Ex :-

Keyword : Play fair
Plain text :- yug Bhavsar

P	L	A	Y	F
I/J	R	B	C	D
E	G	H	K	M
N	O	Q	S	T
U	V	W	X	Z

Plain text :- yu gB HA VS AR

Cipher text :- PX RH BQ OX LB

પ્રશ્ન / પેટા પ્રશ્ન ક્રમાંક Question Sub-question No.	□ + □ + □ + □ = □

Q. 04
Q-A Describe Group and Ring?

Ans-A Group :-

- Set of element on which operation are done (G, ·)

- A Group G is denoted by (G, ·) is a set of operations which are done on set of element that includes to each order pair (a,b) it element in G.

- that associated to each ordered pair (a,b) of elements in G, Group consist following rules

* Theorem ~~(Axioms)~~ Rules

- (A1) closure if a,b ∈ G then a,b ∈ G.
- (A2) Associative: $a*(b*c) = (a*b)*c$
- (A3) Identify Element :- if $a*e = e*a = a$
- (A4) Inverse Element :- if $a'*a = a*a' = e$

* Abelian Group :-

- A group is abelian group if it follows rules

- (A5) Commutation :- if $a*b = b*a$

પ્રશ્ન /
પેટા પ્રશ્ન ક્રમાંક
Question
Sub-question No.

Q.___

Ring :-

- Ring is denoted by R (R, +, *).

- A set of elements with binary two operation addition and multiplication such that for A, B, C ∈ R and following rules are :-

(i) (M1) closure and multiplication : if $a, b \in R$ than $ab \in R$.

(ii) (M2) Associativity of multi : $a(bc) = (ab)c$

(iii) (M3) Distributive law :- $a(b+c) = ab + ac$, $a, b, c \in R$

(iv) (M4) commutative :- $ab = ba$

(v) (M5) No zero division if $a, b \in R$ such that $ab = 0$.

②

PAGE NO.:
DATE:

Assignment - 1
winter 2019

Name :- yug Bhavsar
E. No. :- 196390316007
Sub :- ENS [Essential of Network Security]
Sub code :- 3351602.

Q-A

Q-B Explain man in middle attack.

Ans-B A man in the middle (MITM) attack is general term for where an attacker places himself in a conversation between a sender and receiver or a user and server/application.

- with the Purpose of eavesdrop as well as able to send false information and or to ~~~~ intercept the data transfered between them.

- In this the hacker embedded himself in a communication and im persuating messages to both sides of the conversation and gain access to Funds.

- The objective of an assault is to take individual data, for example, Login credentials, account subtilits and credit cards.

- Targets are regularly the clients of financial applications, saas organizations, online business destination and different sides where signing in is required

- Data acquired during an assault could be utilized for some reasons, including frauds, unapproved fund transfer or an illegal secret key ~~change~~ change.

Q-C Explain single round of DES algorithm

Ans-C

Q-5

Q-A write Euclidean algorithm for GCD. Give one example of it.

Ans A The Euclidean algorithm

* steps

1 A←a, B←b
2 if B=0 return A = gcd (a,b)
3 B = A mod B
4 A←B
5 B←R
6 Go to step 2.

Ex:- 270, 196 Find GCD

270 = 1 * 196 + 74
196 = 2 * 74 + 48
74 = 1 * 48 + 26
48 = 1 * 26 + 22
26 = 1 * 22 + 4
22 = 5 * 4 + 2
4 = 2 * 2 + 0

Explain ECB block cipher mode operation:

it is the easiest mode of operation.

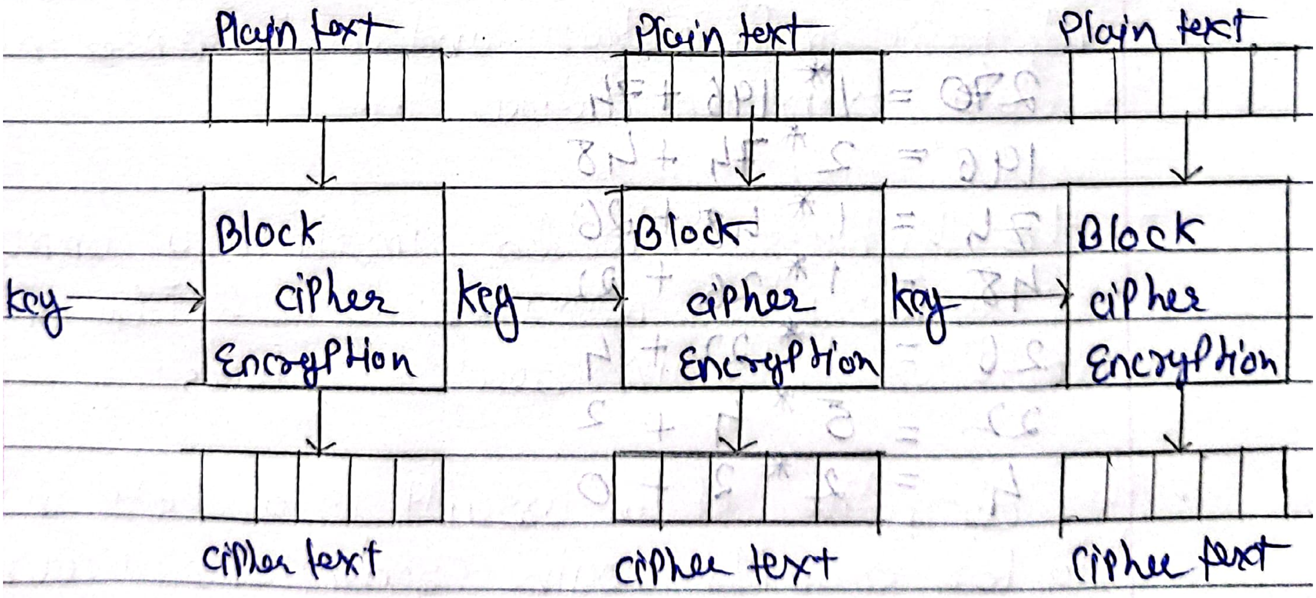
Then entering plain text message is divided into 64 bits block of each

Each block is encrypted independently.

same key is used for all the blocks in the message (encryption)

At the receiver end, incoming data is divided into 64 bits blocks

uses same key for decryption which was used for encryption.



196390316007

PAGE NO.:
DATE:

* Advantages of ECB

- Parallel encryption of Blocks of bits is Possible, thus it is a ~~process~~ faster way of encryption
- Simple way of Block cipher

* Disadvantages of ECB

- Prone to crypt analysis since there is a direct relationship between Plain text and cipher text.

Q-C. Explain cipher Block chaining.

Ans-C.
- it is an advancement made on ECB since ECB compromises some security requirments.
- In CBC, Previous cipher Block is given as input to next encryption algorithm after XOR with ~~algorithm~~ original Plain text block
- In a nut shell here, a cipher block is Produced by encrypting a XOR output of ~~R~~ Previous cipher Block and Present Plain text block.

* Advantages of CBC

- CBC works well for input greater than b bits
- CBC is a good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB

* Disadvantages of CBC

- Parallel encryption is not possible since every encryption requires previous cipher.